

REMARKS

The Examiner has objected to claims 9-13 and 30-34 on the basis that the claims are directed to nonstatutory subject matter. The applicant traverses this objection. The applicant has also amended independent claims 9 and 12 to clarify the scope of protection sought.

The Examiner rejected claims 9-13 on the basis that reference to the element of a “processing unit” in the preamble: a) lacks support in the description; and, b) the preamble is not generally accorded patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness, but, instead, the process steps or structural limitations are able to stand alone.

The applicant respectfully traverses this rejection.

The applicant has further amended the disclosure at page 8 to include a consistory clause that accords with claim 9 as originally filed. The consistory clause includes the element of a processing unit. The applicant further submits that a processing unit is inherent in a computing device executing a cryptographic process and would be self-evident to a person of skill in the art reading the application.

Method claims 9 – 13 as amended relate to a computing device implemented method for executing a countermeasure on a computing device that is intended to execute a defined cryptographic operation. The claimed method steps cover the countermeasure that is implemented by the computing device as an addition/alternative to the defined cryptographic process. The computing device accepts the same input and produces the same output as it would if executing the defined cryptographic process alone, but the computing device is physically transformed when executing the claimed countermeasure.

As is explained in the background of the present application, a “power analysis attack” is a known method for attempting to defeat a cryptographic operation being executed on a computing device. The power analysis attack takes advantage of physical measurements of power levels of various components of the computing device to provide additional information to assist in

defeating the defined cryptographic operation. By measuring the power levels of the device the attacker is able to defeat an otherwise secure cryptographic operation had the attacker only had access to the input and the output from the computing device.

It is known that techniques may be employed to change the operation of the computing device such that the output of the computing device is the same as it would have been had the computing device executed the defined cryptographic operation, but the power levels emitted by the device are changed such that a power analysis attack is less effective.

Some of the known techniques are listed in paragraphs [0007] – [0009]. These known techniques are all for execution on a processing unit of a computing device.

The present application is directed towards a novel split-mask, masking countermeasure that may be implemented by the computing device to supplement a defined cryptographic operation. By executing the countermeasure, the computing device is changed and physical power levels emitted by the device are different from what they would have been had the countermeasure not been implemented.

The applicant submits that the method is tied to a processing unit performing a defined cryptographic function using a key. By implementing the claimed method, power levels in the processing unit are affected such that a power analysis attack on the unit, a physical measurement of the power levels (e.g. a voltage measurement), will be frustrated. There is no purpose to executing the method steps in addition to the defined cryptographic process except to alter the physical characteristics of the computing device executing the countermeasure.

The applicant submits that claims 9-13 as amended are statutory as they are: a) tied to a processing unit that is performing the countermeasure; and, b) the method steps transform the processing unit performing when the countermeasure is executed by altering the resultant power levels to render the processing unit resistant to a power analysis attack. The method alters the operation of the processing unit to change the power levels it emits when it is performing the defined cryptographic operation.

The Examiner objected that the preamble should be given no patentable weight. The applicant respectfully traverses this objection.

The preamble in the present claims is clearly tied to the process and the body of the claim depends upon the recitation that it is a processing unit executing the steps. As explained above, it would be inherent to the person of skill in the art reading the claims and description that a processing unit must carry out the claimed steps to be transformed and rendered resistant to power analysis attacks conducted on that device.

Having regard to claims 30-34, the applicant submits that the claims as previously amended limited the computer program product to one embodied in storage media. The applicant has further deleted the reference to "signals" from the description at page 10 paragraph [0043] for clarity. As previously submitted, in the applicant's view the distinction was clear between signals or embodied in media. The applicant submits that as amended, the application and claims have clearly been limited to statutory subject matter.

"A claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized, and is thus statutory." (MPEP 2106.01)

Favorable consideration and allowance of this application are respectfully requested.

Date: July 29, 2010



---

Etienne P. de Villiers  
Registration No. 58632  
(647) 288-9537

EPdeV:lf